UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,544	01/13/2006	Guy Moreillon	90500-00007S/US	9475

30593   7590   09/29/2008
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER
SHOLEMAN, ABU S

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
09/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/564,544	MOREILLON, GUY
	Examiner	Art Unit	
	ABU SHOLEMAN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>13 January 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-11</u> is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-11</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>13 January 2006</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☒ All   b)☐ Some *   c)☐ None of:

         1.☒ Certified copies of the priority documents have been received.

         2.☐ Certified copies of the priority documents have been received in Application No. _____.

         3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>01/13/2006</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This instant application having Application No. 10564544 filed on

01/13/2006 is presented for examination by the examiner.

Oath/Declaration

2.   The applicants' oath/declaration has been reviewed by the examiner and

is found to conform to the requirements prescribed in **37 C.F.R.1.63.**

Priority

3.   As required by **M.P.E.P.201.14(c),** acknowledgement is made of

applicant's claim for priority based on applications filed on July 14, 2003

(SWITZERLAND 01233/03).

Drawings

The drawings were received on 01/13/2006. These drawings are acceptable for

examination purposes.

Information Disclosure Statement

4.   The information disclosure statement (IDS) submitted on 01/13/2006. The

submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the

information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

5.   Claim 4 recites the limitation "the pseudo-random" in line2. There is

insufficient antecedent basis for this limitation in the claim.

6.   Claim 5 recites the limitation "the master module" in line 3. There is

insufficient antecedent basis for this limitation in the claim.

7.   Claim 6 recites the limitation "the master module" in line 2. There is

insufficient antecedent basis for this limitation in the claim.

8.   Claim 8 recites the limitation "the user security modules" in line2. There is

insufficient antecedent basis for this limitation in the claim.

9.   Claim 9 recites the limitation "the user security modules" in line2. There is

insufficient antecedent basis for this limitation in the claim.

10.   Claim 10 recites the limitation "the master module" in line 3. There is

insufficient antecedent basis for this limitation in the claim.

11.   Claim 11 recites the limitation "the master module identifier" in line2.

There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

12.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13.   Claims 1 are rejected under 35 U.S.C 102(b) as being anticipated by

MAS RIBES et al (WO 03/001807)(hereinafter MAS).

    As per claim 1, MAS discloses "Method for creating and managing a local

network" as (page 1,line 6-9,conditional access system of content, content

distributor and reception with a set-top box), "this network comprising at least

one restitution device for an encrypted data stream" as (page 1, line 4-5, the

conditional access processing of encrypted data such as cable video)and "a

diffusion and re-encrypting device for all or part of said encrypted data" as (

page 2, line 1-2, the broadcasted flow must address every individual decoder at a

receiver level),"said devices comprising security modules" as (page 1, line 9,a

set-top box with a conditional access module), the method comprising the

following steps:

"connecting a master security module in one of the devices connected to

the local network" as(page 3, line 13-14, a secure cryptographic module of a

smart card to the final destination device)," establishing a network key by the

master security module" as(page 1, line 13, the scrambling module at the

distributor uses keys), " securely transmitting this network key to one or several

user security modules" as (page 2, line 17-18, the transmission from the content

protector to the intermediate receiver of said encrypted key or keys),"decrypting

encrypted data by the diffusion and re-encrypting device "as (page2,line 19,the

decryption and re-encryption of said key or keys by the intermediate receiver), "

re-encrypting of the data by said device with a local key" as(page 2, line 28-29,

re-encrypts said content key with a public key of the final destination),

"transmitting the re-encrypted data to the restitution device" as(page 2 , line 20,

the transmission of the re-encrypted key to the final destination), " decrypting by

said restitution device thanks to the associated user security module, which

disposes of means to find the local key" as(page 2, line 21-23, the decrypting of

said re-encrypted key by the final destination and wherein the digital content is

once encrypted for protection by the content protector and once decrypted by

the final destination).

Claim Rejections - 35 USC § 103

14.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described
> as set forth in section 102 of this title, if the differences between the subject matter sought to
> be patented and the prior art are such that the subject matter as a whole would have been
> obvious at the time the invention was made to a person having ordinary skill in the art to which
> said subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

15.   Claims 2 ,3,5,10,11 are rejected under 35 U.S.C.103(a) as being

unpatentable over MAS RIBES et al (WO 03/001807)(hereinafter MAS) in view

of Tararoukhine et al (WO 01/67705)(hereinafter Tararoukhine).

        As per claim 2, MAS RIBES discloses "method for creating and

managing a local network according to claim 1" as (see rejection above claim 1),

But fails to disclose "Wherein the local key is a randomly generated session key

encrypted by the network key" .

        However, Tararoukhine discloses "Wherein the local key is a randomly

generated session key encrypted by the network key" as (page 6, line 4-5,

unique symmetric key encrypted by the different public key for each/all users).

        MAS and Tararoukhine are analogous arts because they are the same

filed of endeavor of apparatus of data access and management system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including a randomly generated public key to access a local network content that taught by Tararoukhine in order to handle the sharing of encrypted files among many users(page 6, line 2-3).

As per Claim 3, MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1), but fails to disclose " Wherein the local key is the network key".

However, Tararoukhine disclose " Wherein the local key is the network key" as (page 5, line 4-5, the different public key for each /all users that is local key as a network key).

MAS and Tararoukhine are analogous arts because they are the same filed of endeavor of apparatus of data access and management system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including the public key to access a local network content that taught by Tararoukhine it would provide speed and efficiency that is required for elegant re-encryption or sharing of encrypted data activity(page 5, line 23-24).

As per claim 5, MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1),

but fails to disclose "wherein the establishment of the network key is carried out during an initialization step of the master module".

However,Tararoukhine discloses "wherein the establishment of the network key is carried out during an initialization step of the master module" as (page 10, line 19-21, using the data encryption and transfer module can be stored on the server computing system such that it can only be accessed by that user who has the establishment of the network key during the initialization step of the master module in the server).

MAS and Tararoukhine are analogous arts because they are the same filed of endeavor of apparatus of data access and management system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including the initialization of the public key that stored in the server that taught by Tararoukhine it would provide all users in the network to accessed of network content.(page 10, line 19-23).

As per claim 10, MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1), but fails to disclose "wherein the diffusion and re-encrypting device includes a security module, called converter module, said module receives and keeps an identifier of the master module that created the network, the converter module re-encrypting the data for a said network".

However, Tararoukhine discloses "wherein the diffusion and re-encrypting device includes a security module, called converter module, said module receives and keeps an identifier of the master module that created the network, the converter module re-encrypting the data for a said network" as (page 8, line 10-23, it will decrypt the key and re-encrypt it with projector's public key. The projector will ready to receive the encrypted movie, decrypt it with key and project it).

MAS and Tararoukhine are analogous arts because they are the same filed of endeavor of apparatus of data access and management system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including the decoder decrypt the data and re-encrypt it for a display that taught by Tararoukhine it would provide all users to securely to manage the data in the network management system (page 8, line 5-8).

As per claim 11,Tararoukhine discloses " wherein said master module identifier is transmitted to a management center during a connection step to said management center" as (page 60, line 17-22, the data encryption and transfer module encrypts the login password and then sends it to the sever).

16.   Claims 4 ,6,7,8 and 9 are rejected under 35 U.S.C.103(a) as being unpatentable over MAS RIBES et al (WO 03/001807)(hereinafter MAS) in view of MARSH David (WO 00/57636)(hereinafter Marsh).

As per claim 4, MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1), but fails to disclose "wherein the establishment of the network key is obtained by the pseudo-random generation of a key during the initialization of the local network".

However, Marsh discloses "wherein the establishment of the network key is obtained by the pseudo-random generation of a key during the initialization of the local network" as (page 20, line 16-18, the random number was properly digital signed with the private key of key pair which is a network).

MAS and Marsh are analogous arts because they are the same filed of endeavor of data encryption and transfer system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including a digital signed network key for a local network that taught by Marsh in order to enhancing smart card usage for associating media content with users in the network (page3, line 6-9).

As per claim 6, MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1), but fails to disclose wherein the master module is placed in a removable security module.

However, Marsh discloses "wherein the master module is placed in a removable security module" as (page 21, line 20-22, smart card is removed from the system which is a removable security module).

MAS and Marsh are analogous arts because they are the same filed of endeavor of data encryption and transfer system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including a smart card in the set-up box that taught by Marsh it would provide more security on the data of smart card by removing from the system (page 21, line 19-21).

As per claim 7, Marsh discloses "wherein said removable security module comprises a user module forming part of the network administrated by the master module" as (page 4, line13-18, a computing devices that a smart card coupled to them (inserted into a smart card reader) this computing device to which a smart chard is coupled to the network).

As per claim 8, MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1), but fails to disclose" wherein the user security modules are in the form of an electronic circuit mounted during the manufacture of the restitution device".

However, Marsh discloses " wherein the user security modules are in the form of an electronic circuit mounted during the manufacture of the restitution device" as (page 15, line 15-18, smart card is an integrated circuit card which is typically the size of a standard credit card and which is capable of storing data and performing some processing).

MAS and Marsh are analogous arts because they are the same filed of endeavor of data encryption and transfer system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including a smart card is mounted into the set-up box that taught by Marsh it would provide more security for content protection controller module includes various functionality to facilitate the protection of media content in the system (page 15, line 22-23).

As per claim 9,MAS RIBES discloses "method for creating and managing a local network according to claim 1" as (see rejection above claim 1), but fails to disclose "wherein the user security module is in the form of a removable security module".

However, Marsh discloses "wherein the user security module is in the form of a removable security module" as (page 13, line 10-15, set-up box may remove scrambling by the transmitter based on a smart card).

MAS and Marsh are analogous arts because they are the same filed of endeavor of data encryption and transfer system.

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of MAS by including a smart card is removable from the set-up box of the system in network that taught by Marsh it would provide more security on the data of smart card by removing from the system(page 21, line 19-21).

Conclusion

17.   The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

18.   The following reference teaches execution of trial data.

    US 2002/0191548

    US 4649233

    US 6993137

    US 2007/0088960

    US 4227253

    US 4933971

    WO 03/001807

    WO 0167705

    WO 00/57636

    Smart card content security

19.   Any inquiry concerning this communication or earlier communication form

the examiner should be directed to Abu Sholeman whose telephone number is (

571)270-7314. the examiner can normally be reached on Monday to Friday 8:30

AM to 5.00PM.

        If attempts to reach the above noted Examiner by telephone are un

successful, the Examiner's supervisor, Thomas Pham, can be reached at the

following telephone number (571)2272-3689.

        The fax phone number for the organization where this application or

proceeding is assigned is 571-273-8300. Information regarding the status of an

application may be obtained from the Patent Application Information Retrieval

(PAIR) system. Status information for published applications may be obtained

from the either Private PAIR or public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about

the PAIR system, see http://pari-direct.uspto.gov. Should your have questions on

access to the Private PAIR system, contact the Electronic Business Center(EBC)

at 866-217-9197(toll-free).

September 18, 2008   Abu Sholeman
                                            Examiner
                                            Art Unit 4148

/Thomas K Pham/

Supervisory Patent Examiner, Art Unit 4148